January 14, 2015

Via Certified Mail and E-Mail

The Honorable Tom Malinowski
Assistant Secretary, Bureau of Democracy, Human Rights and Labor
U.S. Department of State
Harry S. Truman Building
2201 C Street, NW
Washington, DC 20520

cc: Mr. Scott Busby
Deputy Assistant Secretary, Bureau of Democracy, Human Rights and Labor

cc: Mr. Jason Pielemeier
Special Advisor, Bureau of Democracy, Human Rights and Labor

Re: NSA Surveillance and the Universal Periodic Review ("UPR")

Dear Assistant Secretary Malinowski:

We the undersigned write to highlight to your Bureau that the surveillance activities of the National Security Agency ("NSA") have violated the human rights of both Americans and people around the world, and urge you to address these violations in the U.S. report to the UN Human Rights Council. In particular, we urge you to acknowledge in your report the U.S.'s obligation to safeguard the privacy of communications and data that are within the government's power and effective control, regardless of where they are intercepted. We also urge you to identify the steps that the U.S. will take to bring its surveillance activities in line with domestic and international law.

On September 15, 2014, several groups submitted reports to the Council identifying the inconsistencies between the NSA's surveillance operations and U.S. human rights obligations.[1] Since our submissions in September and the State Department's consultation with civil society groups on national security issues in October, troubling revelations about the scope of the NSA's surveillance operations – and their impact on the rights of potentially millions of people around the world – have continued.[2]

President Obama has acknowledged that U.S. surveillance programs "will only be effective if ordinary citizens in other countries have confidence that the United States respects their privacy, too."[3] But U.S. Congressional efforts to reform surveillance programs, still being debated in both Houses, have largely not addressed the concerns of the global population.[4] Presidential Policy Directive 28 ("PPD-28"), which the President released in January 2014 in part to address this

issue, is a step in the right direction, but suffers from significant shortcomings. Although PPD-28 includes modest restrictions on the use of information, it fails to place concrete restrictions on the acquisition and collection of communications and other personal and sensitive data abroad.[5] Additionally, PPD-28 does not impose adequate restrictions on the retention and sharing of information.[6] In particular, it does not specify controls on information sharing with foreign governments, which may use the information to suppress dissent, discriminate, or commit other human rights abuses.

Thus far, the administration and the intelligence community have provided few concrete details to the public on how PPD-28 will be implemented. The U.S. report presents an opportunity for the government to **clarify what, if anything, has changed in practice to better protect privacy under PPD-28**.

The U.S. government **should also acknowledge that its obligation to safeguard the right to privacy does not terminate at our country's borders**.[7] Consistent with the statements of the Human Rights Committee and the Office of the United Nations High Commissioner for Human Rights, the government should recognize that it has a duty to safeguard the privacy of communications and data within its power and effective control, regardless of where they are intercepted.[8] To meet this obligation for foreign intelligence gathering, particularly under Executive Order 12333, the government should build on authorities articulated in PPD-28 or establish new authorities to at least reflect that it will acquire, analyze, store and share personal data only when the information is necessary for the protection of specifically articulated U.S. national security interests, and only in a manner that produces the least intrusion on rights necessary to secure those interests.

Finally, the executive branch **should continue to work with Congress to encourage the passage of reform legislation.** The State Department should describe in the U.S. report steps the administration has taken to support legislative reform to date, as well as how it will support future Congressional efforts to rein in large-scale surveillance programs, particularly under Section 215 of the USA PATRIOT Act, Section 702 of the FISA Amendments Act and EO 12333. The government should also indicate what steps it intends to take if Congress fails to act. For example, it should explain whether it will renew authorization for bulk metadata collection under Section 215, despite findings from two panels appointed to review NSA surveillance that the program has no unique intelligence value.[9]

As the UPR nears, we look forward to further dialogue with the State Department about how the U.S. can more meaningfully realize its commitment to privacy and human rights in the digital age. We also look forward to the U.S. report, which we hope will recognize the gaps between the NSA's surveillance practices and the U.S.'s human rights obligations, and identify concrete ways to address these gaps. If you have any questions, please e-mail or call Amos Toh at amos.toh@nyu.edu or 646-292-8380.

Sincerely yours,

Access
American Civil Liberties Union
Amnesty International USA
Brennan Center for Justice at New York University School of Law
Center for Democracy and Technology
Human Rights Watch
PEN American Center
Privacy International

---

[1] *See e.g.* BRENNAN CENTER FOR JUSTICE ET AL., NATIONAL SECURITY SURVEILLANCE AND HUMAN RIGHTS IN A DIGITAL AGE: JOINT SUBMISSION TO THE UNITED NATIONS UNIVERSAL PERIODIC REVIEW OF THE UNITED STATES (2014) *available at* http://www.brennancenter.org/sites/default/files/analysis/UPR%20Submission%20091514.pdf; AMERICAN CIVIL LIBERTIES UNION & CENTER FOR DEMOCRACY AND TECHNOLOGY, SECRET SURVEILLANCE: FIVE LARGE- SCALE GLOBAL PROGRAMS: JOINT SUBMISSION TO THE UNITED NATIONS UNIVERSAL PERIODIC REVIEW OF THE UNITED STATES (2014) *available at* https://d1ovv0c9tw0h0c.cloudfront.net/files/2014/09/cdt-aclu-upr-9152014.pdf.

[2] For example, media reports reveal that the NSA spies on hundreds of telephone companies around the world to obtain information about security weaknesses in their cell phone networks that it can exploit for surveillance and also has plans to introduce security vulnerabilities in these networks, which would expose data belonging to millions of customers to rogue governments and criminal hackers. *See* Ryan Gallagher, *Operation Auroragold: How the NSA Hacks Cellphone Networks Worldwide,* INTERCEPT (Dec. 4, 2014), https://firstlook.org/theintercept/2014/12/04/nsa-auroragold-hack-cellphones/.

[3] Presidential Remarks on United States Signals Intelligence and Electronic Surveillance Programs, 2014 DAILY COMP. PRES. DOC. 30 (Jan. 17, 2014) *available at* http://www.gpo.gov/fdsys/pkg/DCPD-201400030/pdf/DCPD-201400030.pdf; Directive on Signals Intelligence Activities: Presidential Policy Directive/PPD-28, 2014 DAILY COMP. PRES. DOC. 31 (Jan. 17, 2014) [hereinafter PPD-28] *available at* http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[4] Although USA FREEDOM Act, the central Congressional reform effort, garnered widespread support, the bill has stalled in Congress, failing to clear a procedural vote in the Senate on November 18, 2014. The bill would, among other things, prohibit the bulk collection of telephone and other records under certain authorities, require the destruction of unrelated information within a reasonable time frame, and facilitate declassification of some opinions of the Foreign Intelligence Surveillance Court. S. 2685, 113th Cong. (2d Sess. 2014) *available at* https://www.congress.gov/113/bills/s2685/BILLS-113s2685pcs.pdf.

[5] Although PPD-28 states that US surveillance activities will not be conducted to suppress dissent or for discriminatory purposes, and will be "as tailored as feasible," the broad range of "foreign intelligence purposes" for which collection is permitted – namely any information relating to the "capabilities, intentions, or activities" of foreign governments ... foreign organizations, foreign *persons*, or international terrorists" – remains unchanged. PPD-28 § 1(b), *id* at §1(d); Exec. Order No. 12, 333, § 3.5(3), 3 C.F.R. 200 (1981 Comp.), *reprinted in* 50 U.S.C § 401 (Supp. V 1981). A broad definition of "foreign intelligence" makes no distinction between the e-mails of foreign students discussing terrorism in the Middle East and those between persons with suspected ties to ISIS.

[6] We welcome the recent announcement that intelligence agencies will no longer "permanently retain or disseminate" any information "*solely* because of the person's non-US status." OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, SAFEGUARDING THE PERSONAL INFORMATION OF ALL PEOPLE: A STATUS REPORT ON THE DEVELOPMENT AND IMPLEMENTATION OF PROCEDURES UNDER PRESIDENTIAL POLICY DIRECTIVE 28, 5 (Jul. 2014) *available at* http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf.

However, we are skeptical of the privacy value of PPD-28's central reform: extending US person dissemination and retention procedures to non-US persons. PPD-28 §4(a)(i). Current procedures for handling US persons' information allow for virtually indefinite retention and widespread sharing of a wide range of data, even if it has little or no intelligence value. For example, the law permits the NSA to keep encrypted communications for however long it takes to decipher them. Intelligence Authorization Act for Fiscal Year 2015, Pub. L. No. 113-293, 128 Stat. 3990 § 309(3)(B)(iii) (2014); OFFICE OF PRIMARY CONCERN, UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE SP0018: LEGAL COMPLIANCE AND U.S. PERSONS MINIMIZATION PROCEDURES, § 6.1(a)

(2011) *available at* http://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf. The vast amounts of data stored on the NSA's databases may also be shared with many US government agencies as long as it is for the performance of a "lawful governmental function." DEPARTMENT OF DEFENSE, ACTIVITIES OF DOD INTELLIGENCE COMPONENTS THAT AFFECT UNITED STATES PERSONS, § C.4.2.2.4, DOD 5240 1-R (1982), *available at* http://dtic.mil/whs/directives/corres/pdf/524001r.pdf. Extending these rules to non-US persons would add little to their privacy.

[7] U.S. recognition of the extraterritorial application of fundamental rights is not unprecedented. For example, in the context of torture, the U.S. has recognized that its obligation to prevent torture and cruel treatment applies in places that it controls "as a governmental authority." Press Release, Office of the Press Secretary, Statement by NSC Spokesperson Bernadette Meehan on the U.S. Presentation to the Committee Against Torture (Nov. 12, 2014) *available at* http://www.whitehouse.gov/the-press-office/2014/11/12/statement-nsc-spokesperson-bernadette-meehan-us-presentation-committee-a.

[8] U.N. H.R.C. Rep. of the Office of the U.N. High Comm'n for Human Rights, ¶ ¶ 32, U.N. DOC. A/HRC/27/37 (June 30, 2014) *available at* http://www.ohchr.org/en/hrbodies/hrc/regularsessions/session27/documents/a.hrc.27.37_en.pdf; United Nations, Human Rights Committee, General Comment 31, Nature of the General Legal Obligation on States Parties to the Covenant, ¶ ¶ 10, U.N. DOC. CCPR/C/21/Rev.1/Add.13 (2004) http://www1.umn.edu/humanrts/gencomm/hrcom31.html.

[9] *See generally* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (2014) *available at* http://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf; *also see* RICHARD A. CLARKE ET AL., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES (2013) *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.